

**DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION**
(The requirements of the DoD Industrial Security Manual apply
to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED

SECRET

b. LEVEL OF SAFEGUARDING REQUIRED

SECRET**2. THIS SPECIFICATION IS FOR: (X and complete as applicable)**

<input checked="" type="checkbox"/>	a. PRIME CONTRACT NUMBER	
	b. SUBCONTRACT NUMBER	
	c. SOLICITATION OR OTHER NUMBER	DUE DATE (YYYYMMDD)

3. THIS SPECIFICATION IS: (X and complete as applicable)

<input checked="" type="checkbox"/>	a. ORIGINAL (Complete date in all cases)	DATE (YYYYMMDD)
	b. REVISED (Supersedes all previous specs)	REVISION NO. DATE (YYYYMMDD)
	c. FINAL (Complete Item 5 in all cases)	DATE (YYYYMMDD)

4. IS THIS A FOLLOW-ON CONTRACT?☐ YES☒ NO

If Yes, complete the following:

Classified material received or generated under _____ (Preceding Contract Number) is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254?☐ YES☒ NO

If Yes, complete the following:

In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____

6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)

a. NAME, ADDRESS, AND ZIP CODE TBD	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) TBD
---------------------------------------	--------------	---

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE TBD	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) TBD
---------------------------------------	--------------	---

8. ACTUAL PERFORMANCE

a. LOCATION TBD	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
--------------------	--------------	--

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

AMCOM Express for Technical, or Programmatic, or Logistics, or Business Analytical Support Services

10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
b. RESTRICTED DATA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	<input checked="" type="checkbox"/>	<input type="checkbox"/>
d. FORMERLY RESTRICTED DATA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	<input checked="" type="checkbox"/>	<input type="checkbox"/>
e. INTELLIGENCE INFORMATION	<input type="checkbox"/>	<input type="checkbox"/>	e. PERFORM SERVICES ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
(1) Sensitive Compartmented Information (SCI)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(2) Non-SCI	<input checked="" type="checkbox"/>	<input type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	<input checked="" type="checkbox"/>	<input type="checkbox"/>
f. SPECIAL ACCESS INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT	<input checked="" type="checkbox"/>	<input type="checkbox"/>
g. NATO INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	i. HAVE TEMPEST REQUIREMENTS	<input type="checkbox"/>	<input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	<input checked="" type="checkbox"/>	<input type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	l. OTHER (Specify)		
k. OTHER (Specify)					

- 12. PUBLIC RELEASE.** Any information (*classified or unclassified*) pertaining to this contract shall not be released for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (*Specify*)

REQUIRING ELEMENT
NO PUBLIC RELEASE OF SAP
INFORMATION IS AUTHORIZED

REQUEST FOR RELEASE OF OTHER THAN
SCI MUST BE APPROVED BY CONTRACTING
OFFICERS REPRESENTATIVE

AMSAM-PA

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

- 13. SECURITY GUIDANCE.** The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (*Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.*)

10a - COMSEC: Requirement is for the purpose of secure communications STU III only.

10e(1) - See enclosure for Sensitive Compartmented security requirements.

10e(2) - See enclosure 2 for Non Sensitive Compartmented Information security requirements

10f - 1. Access to Special Access Program (SAP) information will be granted at approved Government facilities/other contractor facilities only. Security procedures specified at facilities where SAP information is accessed will be followed. Contractor is not authorized to discuss, store, generate, or process SAP information in his facility.

2. Contractor personnel SSBI accessed to SAP information will require minimum of SECRET personnel security clearance based on a current (within 5 years) investigation

3. Contractor personnel accessed to SAP information required in the performance of this contract are subject to random selection for counterintelligence - Scope polygraph examinations in accordance with DoD Directive 5210 48. Failure of selected individuals to submit to polygraph examination may result in access to SA information being suspended.

4. All DD Forms 254 prepared for subcontractors involving access to SAP under this contract effort must be forwarded to SAP Program Manager for review and concurrence prior to the award of the subcontract.

(See continuation page for #13)

- 14. ADDITIONAL SECURITY REQUIREMENTS.** Requirements, in addition to ISM requirements, are established for this contract. ☐ Yes ☒ No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

- 15. INSPECTIONS.** Elements of this contract are outside the inspection responsibility of the cognizant security office. ☐ Yes ☒ No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

- 16. CERTIFICATION AND SIGNATURE.** Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE (Include Area Code)
d. ADDRESS (Include Zip Code)		17. REQUIRED DISTRIBUTION <input checked="" type="checkbox"/> a. CONTRACTOR <input checked="" type="checkbox"/> b. SUBCONTRACTOR <input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR <input type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION <input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER <input checked="" type="checkbox"/> f. OTHERS AS NECESSARY
e. SIGNATURE		

Item 13 Security Guidance (Continuation)

10g. The NISPOM provides instructions for handling NATO and Foreign Government information. The following instructions also apply:

1. NATO material released to the contractor does not become the property of the contractor and may be withdrawn at any time.
2. Upon expiration of the contract all NATO material will be returned to the U.S. Army Aviation and Missile Command NATO Control Officer
3. Your company will not reproduce NATO material released to your custody without the express written permission of the USAAMCOM NATO Control Officer. When written permission is received to reproduce NATO material, your company will control and account for such reproductions in the same manner as pertain to the originals.
4. NATO material released to your company will not be destroyed unless written authorization for such destruction is received from the USAAMCOM NATO Control Officer. In the event such authorization is received, your company will effect such destruction in accordance with the Industrial Security Manual. A copy of the destruction certificate will be sent to USAAMCOM NATO Control Officer, AMSAM-PT-OC.

10 j. Any weapons system security classification guide (SCG) applicable to a given technical direction order will be provided under separate cover. Information generated under this contract will be marked in accordance with source documentations and will be marked as follows:

DERIVED FROM: (Source document, multiple sources, or security classification guide, date and POC)

DECLASSIFY ON: Date/event from source document or "Source Marked OADR"

DATE OF SOURCE: (Date of source document or SCG)

11e. Contractor will be performing graphic arts and engineering services also.

11g. DTIC and RSIC and DoD Information Analysis Centers may be used as a source of Scientific and Technical Information (STINFO) only and will be authorized at the discretion of the Program/Project Manager, DTIC requires contractor to prepare and process DD Form 1540 and DD Form 1541. SAP information will not be released to DTIC or RSIC.

11h. Basic requirement is for STU III COMSEC account only. Additional COMSEC requirements may be required and will be detailed in specific contractual instruments.

11j. The prime contractor and any subcontractors will adhere to the Operational Security (OPSEC) provisions of Army Regulation AR 530-1, OPSEC. No OPSEC plan is required as a deliverable data item.

Each subcontract requiring access to classified information must have a DD254, and will be reviewed by ISD/AMCOM.

Classification guidance must be provided in accordance with AR 380-5, and Executive Order 12958.

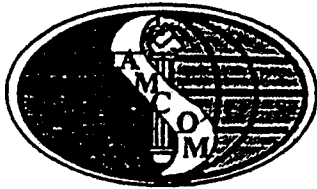
Item 14 Additional Security Requirements (Continuation)

Personnel accessed to a Special Access Program (SAP) must comply with the provisions of the NISPOM SAP Supplement, the DOD Overprint to the NISPOM SAP Supplement, the Program Security Procedures Guide and the Program Security Classification Guide. Access will be granted only at Government or contractor facilities approved by the SAP program manager. The Program SPG and SCG will be available at the facility where access is granted.

Instructions for Completion of AMSAM-SI-F FORM 1

1. Fill in all blanks.
2. If contract is a follow-on or extension, place old contract number to the right of the block checked.
3. State the purpose of the contract and how the intelligence information will be used in the block "purpose of contract."
4. In the block "responsible Government office," put in the command contracting organization. For AMCOM and supported organizations, this will be the AMCOM Acquisition Center. Put in the name, office symbol, and telephone number of the contract administrator from the Acquisition Center responsible for the applicable contract.
5. The contract monitor in the responsible Government office must be shown and his signature must appear in the last block.
6. This form must be completed and received by the foreign intelligence division prior to any release of intelligence material, written or oral, to the contractor.
7. Eligibility for receipt of intelligence material must be granted on a contract-by-contract and task order basis.
8. Execution of this form and its filing with the Foreign Intelligence Division certifies the contractor's need-to-know for this contract.
9. The contract monitor must identify the required intelligence material to be forwarded to the contractor on the request for release form (usually assisted by FID representative). For documents, this should be by title, if known. If unknown, or for other products/information, a short description will suffice.
10. The FID will forward all intelligence materials to the contractor.
11. It shall be understood that an automatic suspense date of 90 days from receipt will be imposed unless designated otherwise by the contract monitor.
12. Any extension of the use of these materials or transfer to another contract must be requested from the FID by the contract monitor.

Authority: AR 381-1



FOREIGN INTELLIGENCE

FOREIGN INTELLIGENCE DIVISION

CONTRACTOR'S ELIGIBILITY TO
RECEIVE
INTELLIGENCE MATERIAL

CONTRACT/RFP TITLE NUMBER		<input type="checkbox"/> NEW <input type="checkbox"/> EXTENSION <input type="checkbox"/> FOLLOW-ON	
CONTRACTOR NAME		EFFECTIVE DATES OF CONTRACT	
SECURITY OFFICER		FROM	TO
MAILING ADDRESS		FACILITY CLEARANCE	
TELEPHONE NUMBER		DATE GRANTED AND BY WHOM	
		STORAGE CAPABILITY	
PURPOSE OF CONTRACT AND INTELLIGENCE UTILIZATION			
RESPONSIBLE GOVERNMENT OFFICE		TECHNICAL MONITOR	
CONTRACT ADMINISTRATOR		OFFICE SYMBOL	PHONE
OFFICE SYMBOL	PHONE	SIGNATURE	DATE

DATE _____

CONTRACT NO.

Signature: _____
Contract Monitor

[illegible]

SECURITY REQUIREMENTS FOR INTELLIGENCE INFORMATION(encl 2)

1. Intelligence material released under this contract or Request for Proposal remains the property of the United States Government and may be withdrawn upon notice.
2. A record will be maintained of all the classified intelligence material released to your custody. Unclassified material will be treated as FOUO.
3. All reproductions of intelligence will be classified, marked, and controlled in the same manner as original(s).
4. Prior to granting an employee access to intelligence materials, employees will be briefed on their obligation to comply with these procedures and will be debriefed when access to the material is terminated. A permanent list of all employees having had access to the intelligence materials during this contract will be maintained by the company and will be available for DIS inspection.
5. You will not release intelligence material to any activity, employee, or other person not directly engaged in providing services under this contract unless specific written authorization for such release is received from the releasing organization. This prohibition precludes release without authority to another contractor, Government agency, private individual, or organization unless a contractual relationship exists. Specific written authorization for such release will be received from Commander, U.S. Army Aviation and Missile Command, ATTN: AMSAM-SI-FO, RSA, AL 35898-5000.
6. The intelligence materials will not be released to foreign nations, non-U.S. citizens or U.S. citizens representing foreign entities except with specific written authorization from this office, whether or not they are consultants, a U.S. contractor or employees of a contractor, and regardless of the level of their access authorization.
7. Intelligence materials released to you will not be destroyed unless permission is received for internally generated or extracted intelligence materials. In the event the contract is extended or a new similar contract requiring the released data is initiated, it is the responsibility of the contract monitor to effect an extension or document transfer with the issuing agency.

GUIDANCE FOR THE PROTECTION OF "FOR OFFICIAL USE ONLY" (FOUO) INFORMATION (encl 3)

1. General. The "FOR OFFICIAL USE ONLY" (FOUO) marking is assigned to information at the time of its creation. It is used to designate official government information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act. Use of the marking does not mean that the information cannot be released to the public, only that it must be reviewed by the government prior to its release to determine whether a significant and legitimate government purpose is served by withholding the information or portions of it.
2. Identification Markings.
 - a. An unclassified document containing FOUO information will be marked "FOR OFFICIAL USE ONLY" at the bottom of the front cover (if any) on the first page, on each page containing FOUO information, on the back page, and on the outside of the back cover (if any). No portion markings will be shown.
 - b. Within a classified document an individual page that contains both FOUO and classified information will be marked at the top and bottom with the highest security classification of information appearing on the page. If an individual portion contains FOUO information but no classified information, the portion will be marked, FOUO.
 - c. Any "FOR OFFICIAL USE ONLY" information released is required to be marked with the following statement prior to transfer: *This document contains information EXEMPT FROM MANDATORY DISCLOSURE under FOIA, Exemptions _____ apply.*
 - d. Removal of the "FOR OFFICIAL USE ONLY" marking can only be accomplished by the originator or other competent authority. When the "FOR OFFICIAL USE ONLY" status is terminated, all known holders will be notified to the extent possible.
3. Dissemination. "FOR OFFICIAL USE ONLY" Information may be disseminated by contractors to their employees and subcontractors who have a need for the information in connection with a classified contract.
4. Storage. During working hours, "FOR OFFICIAL USE ONLY" information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During non-working hours, the information shall be stored to preclude unauthorized access. Filing such material with other unclassified information in unlocked files or desks, is adequate when internal building security is provided during non working hours. When such internal security control is not exercised, locked buildings or rooms will provide adequate after-hours protection or the material can be stored in locked receptacles such as file cabinets, desks, or bookcases.
5. Transmission. "FOR OFFICIAL USE ONLY" information may be sent via first-class mail or parcel post. Bulky shipments may be sent by fourth-class mail.
6. Disposition. When no longer needed, "FOR OFFICIAL USE ONLY" information may be disposed by tearing each copy into pieces to preclude reconstruction and placing it in a regular trash container.
7. Unauthorized Disclosure. Unauthorized disclosure of "FOR OFFICIAL USE ONLY" does not constitute a security violation but the contracting officer should be informed of any unauthorized disclosure. The unauthorized disclosure of "FOR OFFICIAL USE ONLY" information protected by the Privacy Act may result in criminal sanctions.